FIG. 1

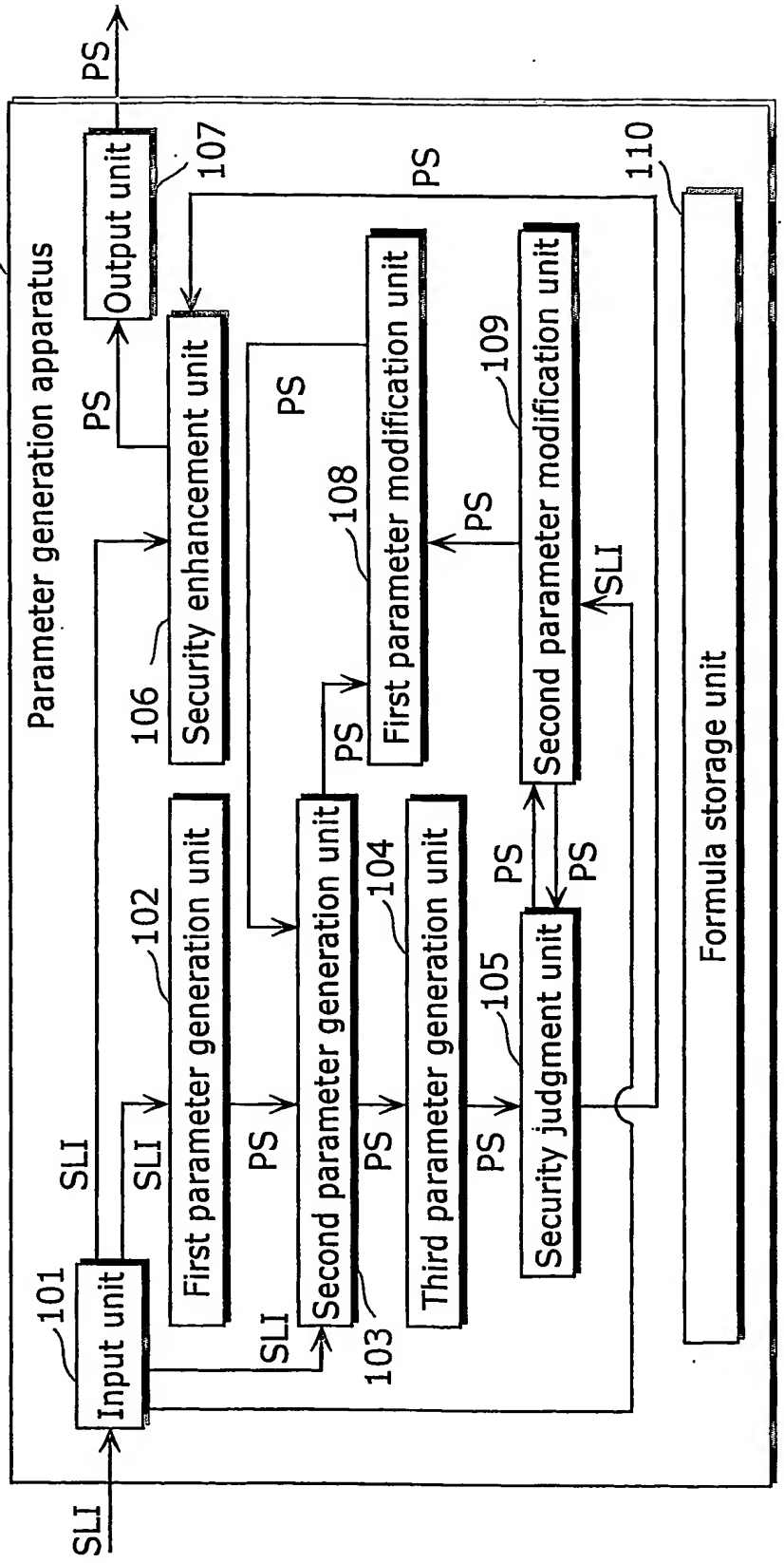

1
Parameter generation apparatus
Input unit
101
First parameter generation unit
102
Second parameter generation unit
103
Third parameter generation unit
104
Security judgment unit
105
Security enhancement unit
106
Output unit
107
First parameter modification unit
108
Second parameter modification unit
109
Formula storage unit
110
SLI
PS

FIG. 2

Parameter N	Decryption time T (seconds)
70	16.587
72	18.68
74	26.497
76	25.869
78	31.182
80	37.76
82	56.442
84	56.359
86	68.174
88	86.6
90	111.78

FIG. 3

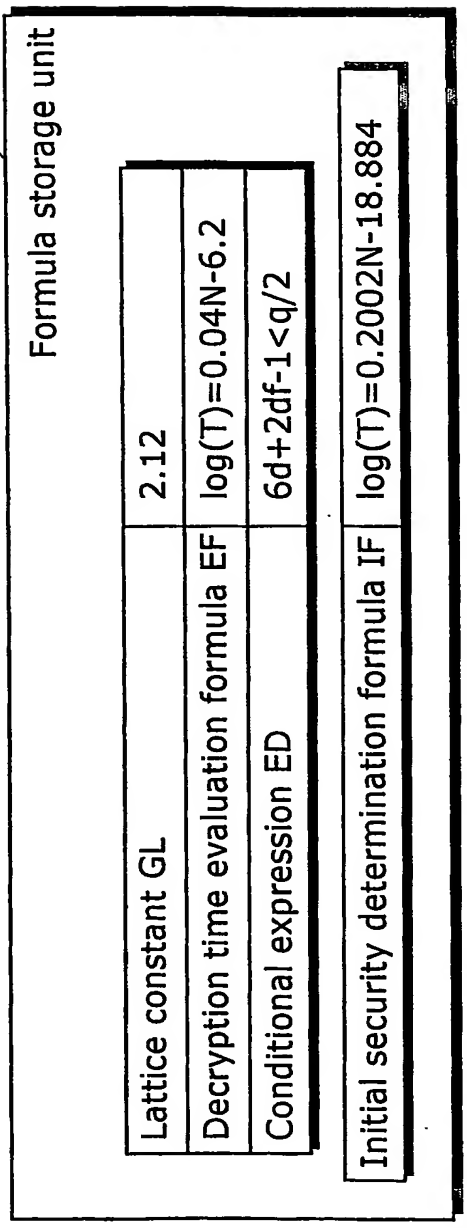

110
Formula storage unit
Lattice constant GL
2.12
Decryption time evaluation formula EF
log(T)=0.04N-6.2
Conditional expression ED
6d+2df-1<q/2
Initial security determination formula IF
log(T)=0.2002N-18.884

FIG. 4

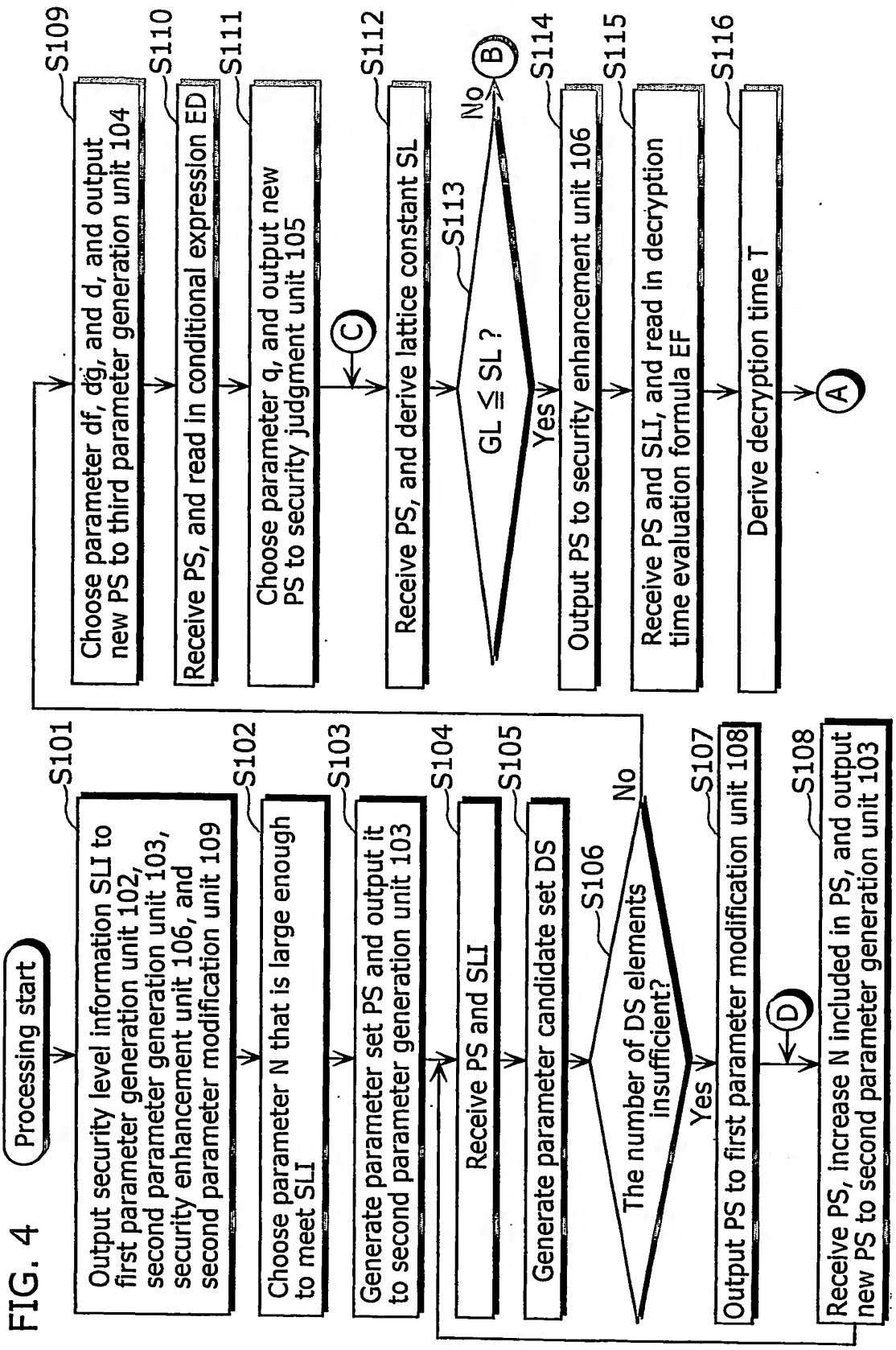

Processing start
S101
Output security level information SLI to first parameter generation unit 102, second parameter generation unit 103, security enhancement unit 106, and second parameter modification unit 109
S102
Choose parameter N that is large enough to meet SLI
S103
Generate parameter set PS and output it to second parameter generation unit 103
S104
Receive PS and SLI
S105
Generate parameter candidate set DS
S106
The number of DS elements insufficient?
No
Yes
S107
Output PS to first parameter modification unit 108
D
S108
Receive PS, increase N included in PS, and output new PS to second parameter generation unit 103
C
S109
Choose parameter df, dg, and d, and output new PS to third parameter generation unit 104
S110
Receive PS, and read in conditional expression ED
S111
Choose parameter q, and output new PS to security judgment unit 105
S112
Receive PS, and derive lattice constant SL
S113
GL ≦ SL ?
No
B
Yes
S114
Output PS to security enhancement unit 106
S115
Receive PS and SLI, and read in decryption time evaluation formula EF
S116
Derive decryption time T
A

FIG. 5

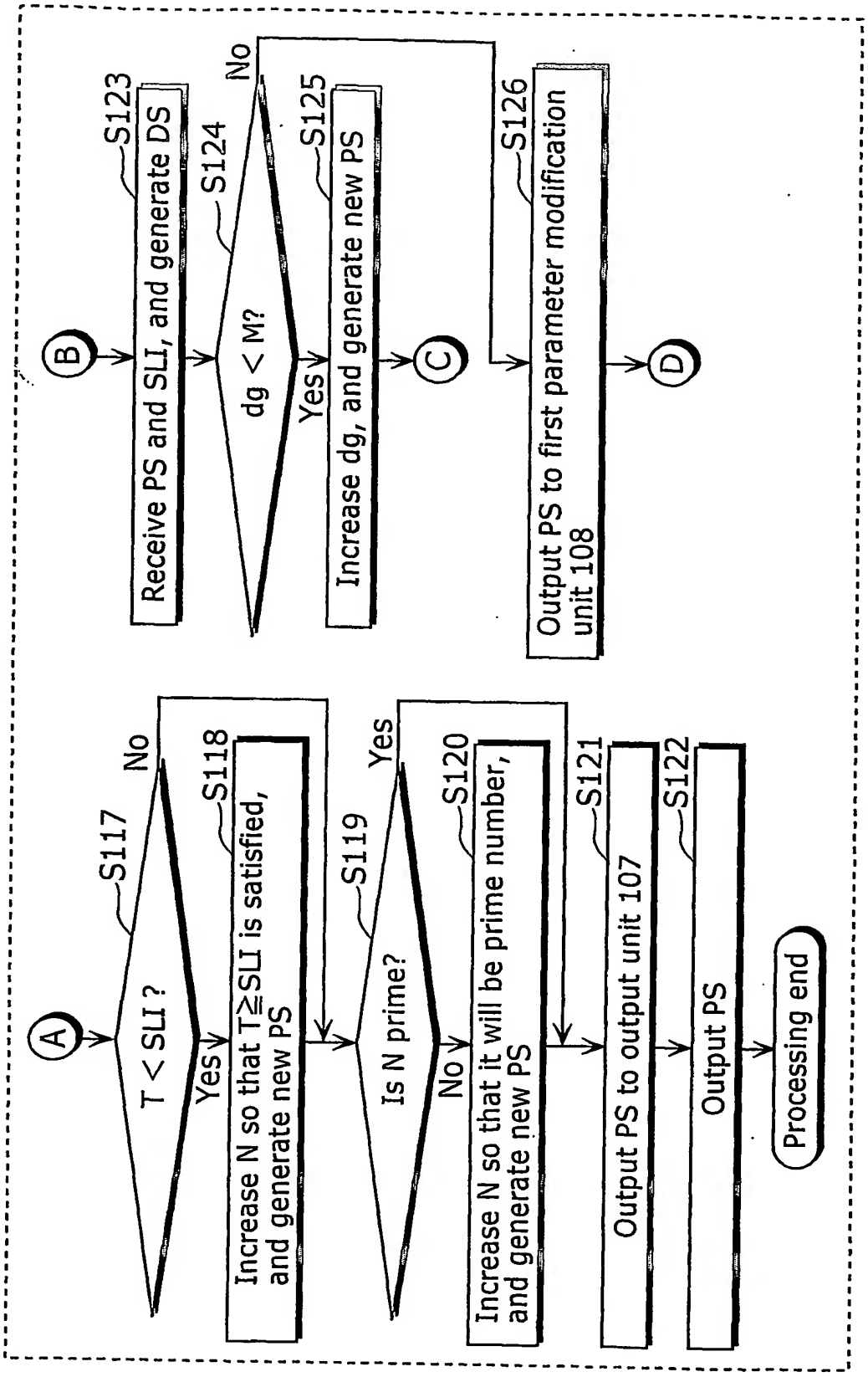

A
S117
T < SLI ?
No
Yes
S118
Increase N so that T≧SLI is satisfied, and generate new PS
S119
Is N prime?
Yes
No
S120
Increase N so that it will be prime number, and generate new PS
S121
Output PS to output unit 107
S122
Output PS
Processing end
B
S123
Receive PS and SLI, and generate DS
S124
dg < M?
No
Yes
S125
Increase dg, and generate new PS
C
S126
Output PS to first parameter modification unit 108
D

FIG. 6

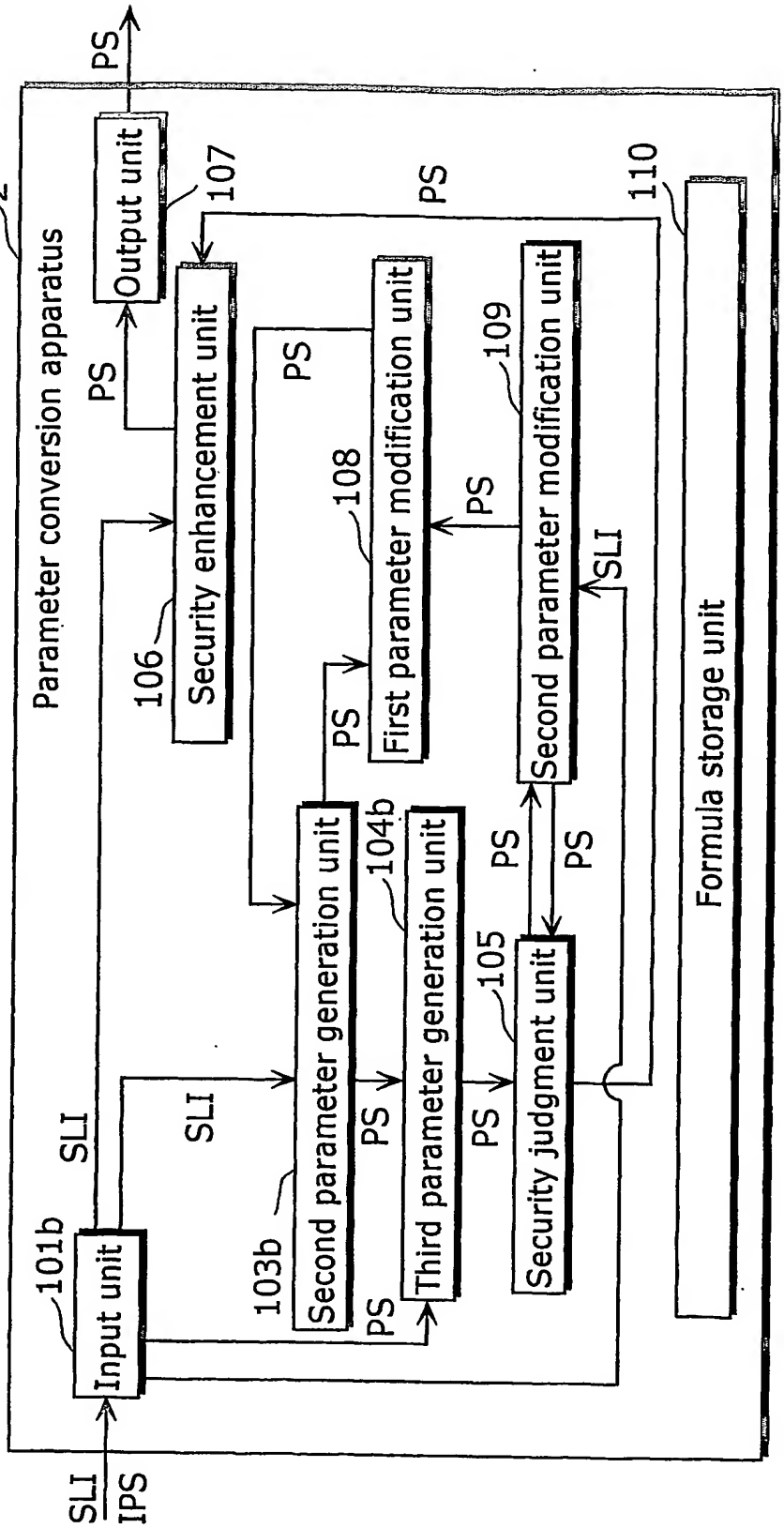

2
Parameter conversion apparatus
Output unit
107
PS
110
Formula storage unit
Security enhancement unit
106
First parameter modification unit
108
Second parameter modification unit
109
SLI
Second parameter generation unit
103b
Third parameter generation unit
104b
Security judgment unit
105
Input unit
101b
SLI
IPS

FIG. 7

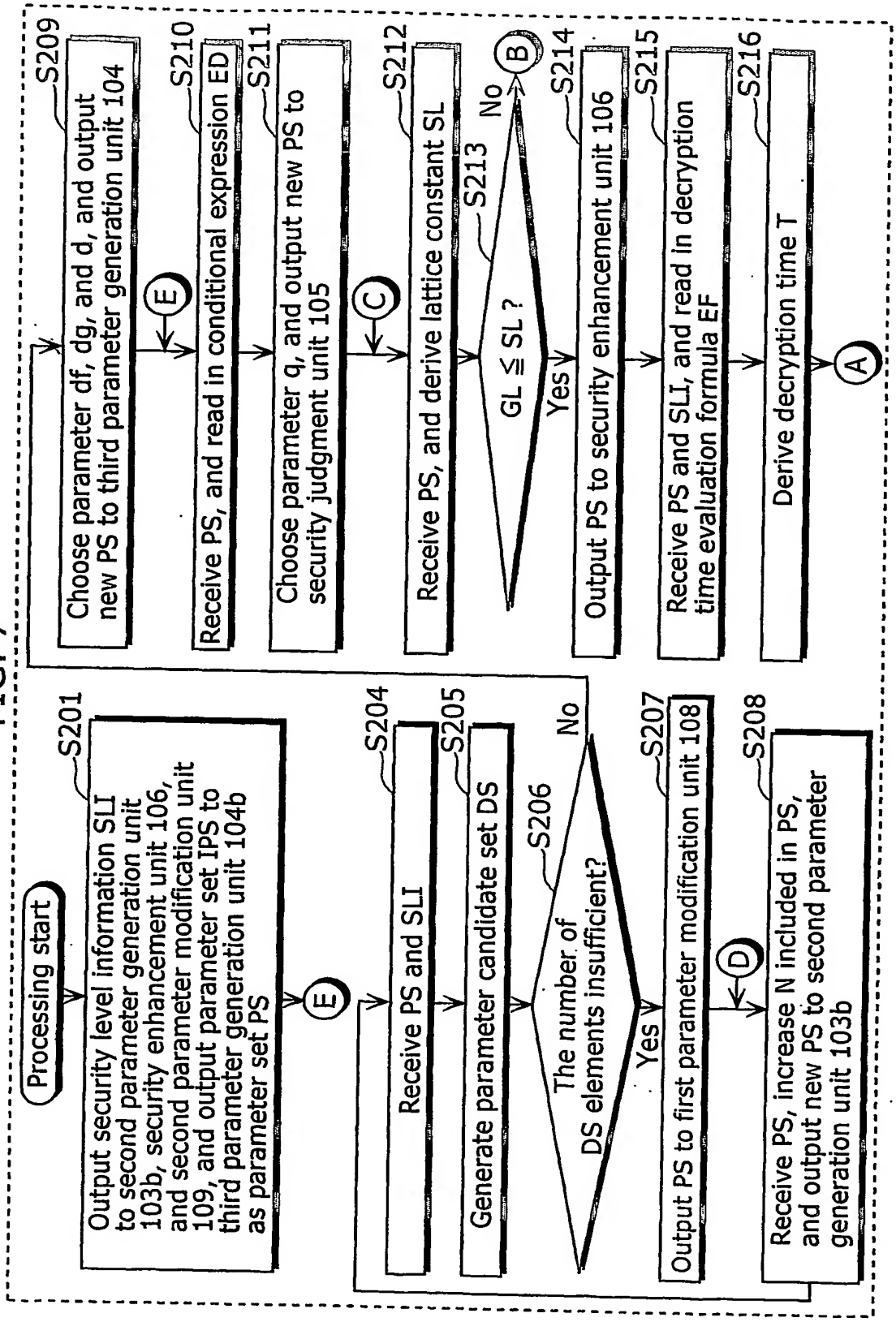

Processing start
S201
Output security level information SLI to second parameter generation unit 103b, security enhancement unit 106, and second parameter modification unit 109, and output parameter set IPS to third parameter generation unit 104b as parameter set PS
E
S204
Receive PS and SLI
S205
Generate parameter candidate set DS
S206
The number of DS elements insufficient?
No
Yes
S207
Output PS to first parameter modification unit 108
D
S208
Receive PS, increase N included in PS, and output new PS to second parameter generation unit 103b
S209
Choose parameter df, dg, and d, and output new PS to third parameter generation unit 104
E
S210
Receive PS, and read in conditional expression ED
S211
Choose parameter q, and output new PS to security judgment unit 105
C
S212
Receive PS, and derive lattice constant SL
S213
GL ≦ SL ?
No
B
Yes
S214
Output PS to security enhancement unit 106
S215
Receive PS and SLI, and read in decryption time evaluation formula EF
S216
Derive decryption time T
A

FIG. 8

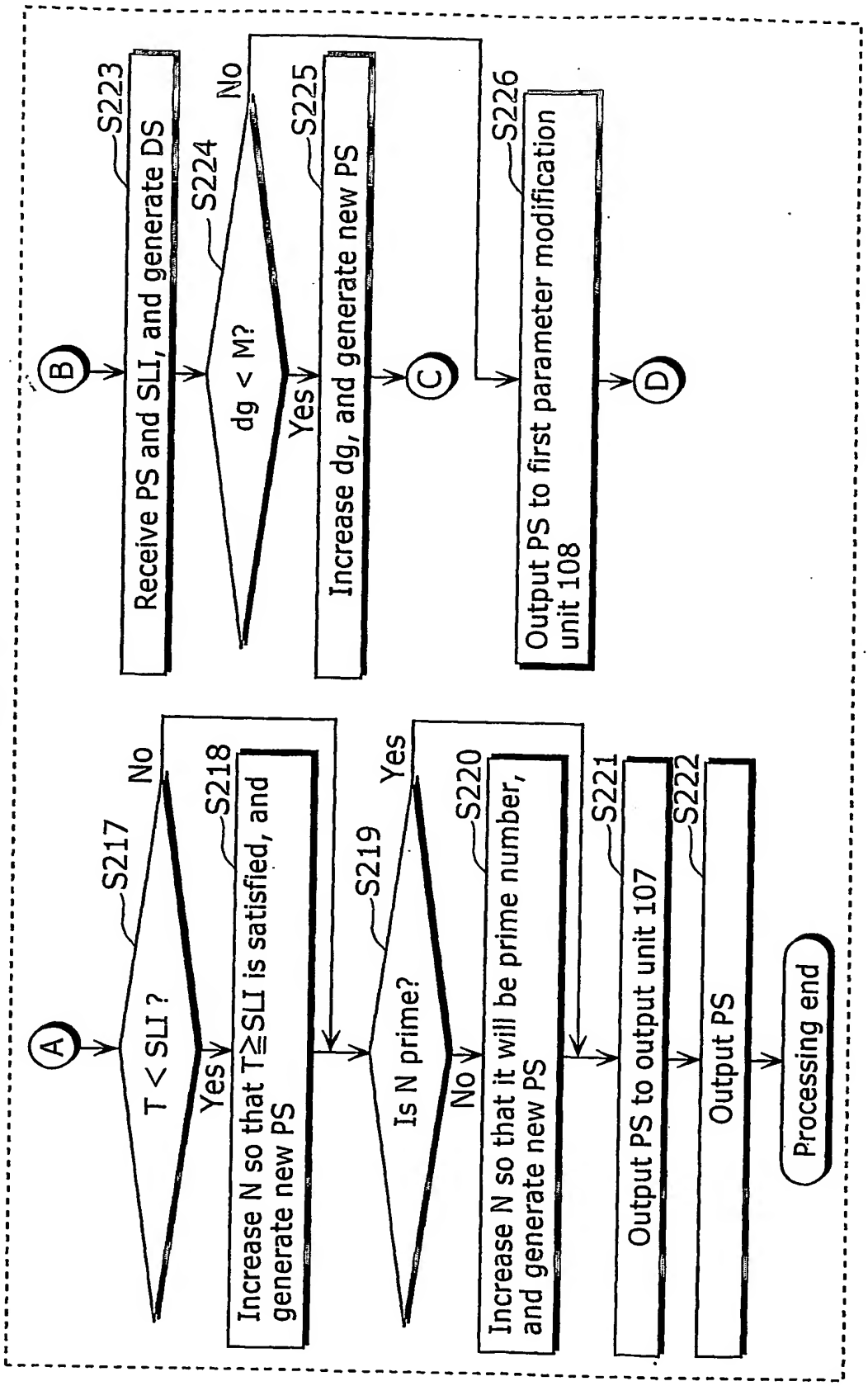

A
S217
T < SLI ?
No
Yes
S218
Increase N so that T≧SLI is satisfied, and generate new PS
S219
Is N prime?
Yes
No
S220
Increase N so that it will be prime number, and generate new PS
S221
Output PS to output unit 107
S222
Output PS
Processing end
B
S223
Receive PS and SLI, and generate DS
S224
dg < M?
No
Yes
S225
Increase dg, and generate new PS
C
S226
Output PS to first parameter modification unit 108
D

FIG. 9

Security level information SLI	Parameter set IPS
For 512-bit RSA encryption	IPS=(167, 3, 128, 61, 280, 18)
For 1024-bit RSA encryption	IPS=(263, 3, 128, 50, 24, 16)
For 2048-bit RSA encryption	IPS=(503, 3, 256, 217, 72, 55)
:	:

FIG. 10

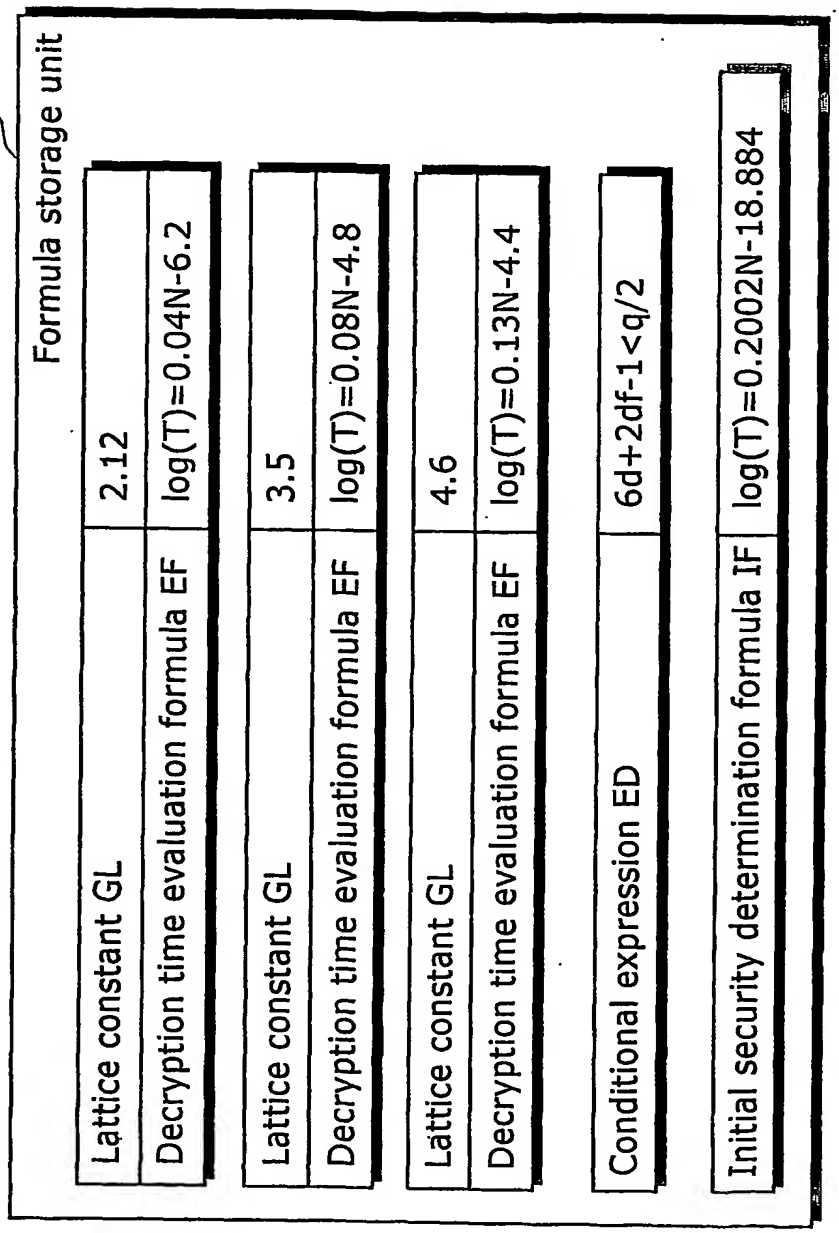

110
Formula storage unit
Lattice constant GL
2.12
Decryption time evaluation formula EF
log(T)=0.04N-6.2
Lattice constant GL
3.5
Decryption time evaluation formula EF
log(T)=0.08N-4.8
Lattice constant GL
4.6
Decryption time evaluation formula EF
log(T)=0.13N-4.4
Conditional expression ED
6d+2df-1<q/2
Initial security determination formula IF
log(T)=0.2002N-18.884

FIG. 11

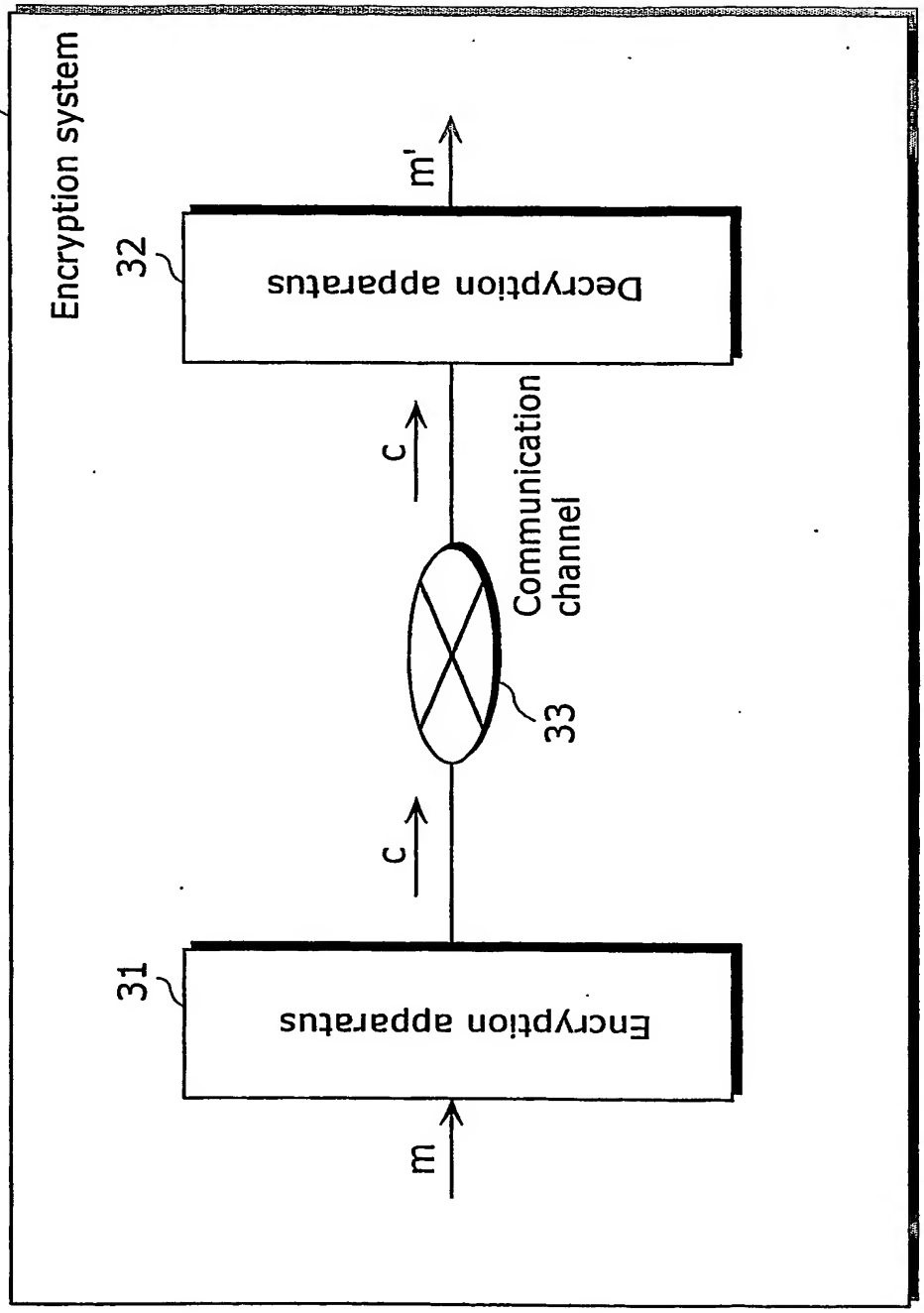

3
Encryption system
32
Decryption apparatus
m'
c
Communication channel
33
c
31
Encryption apparatus
m

FIG. 12

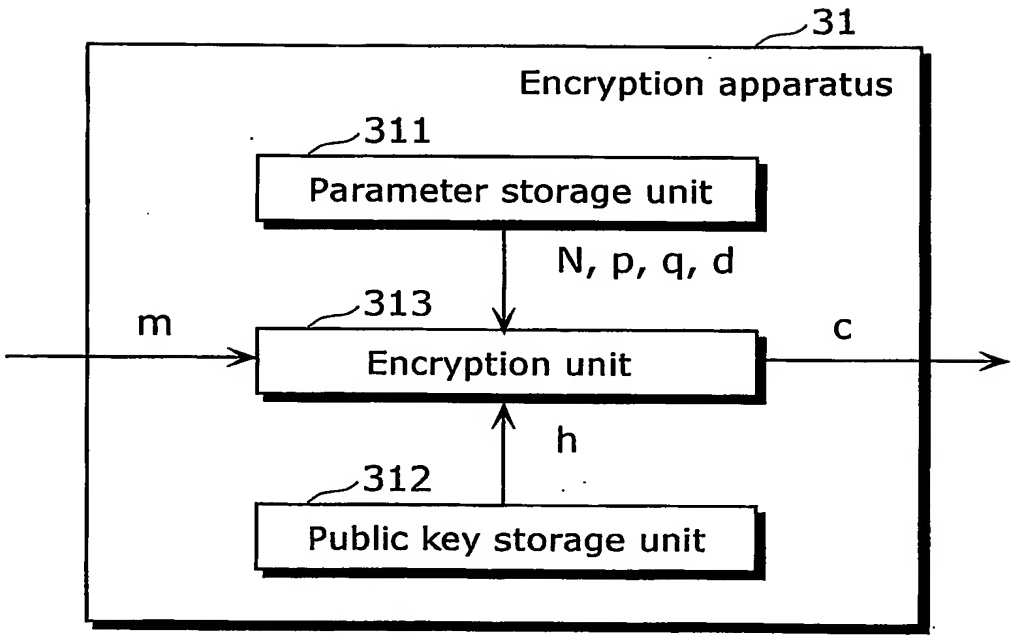

31
Encryption apparatus
311
Parameter storage unit
N, p, q, d
313
m
c
Encryption unit
h
312
Public key storage unit

FIG. 13

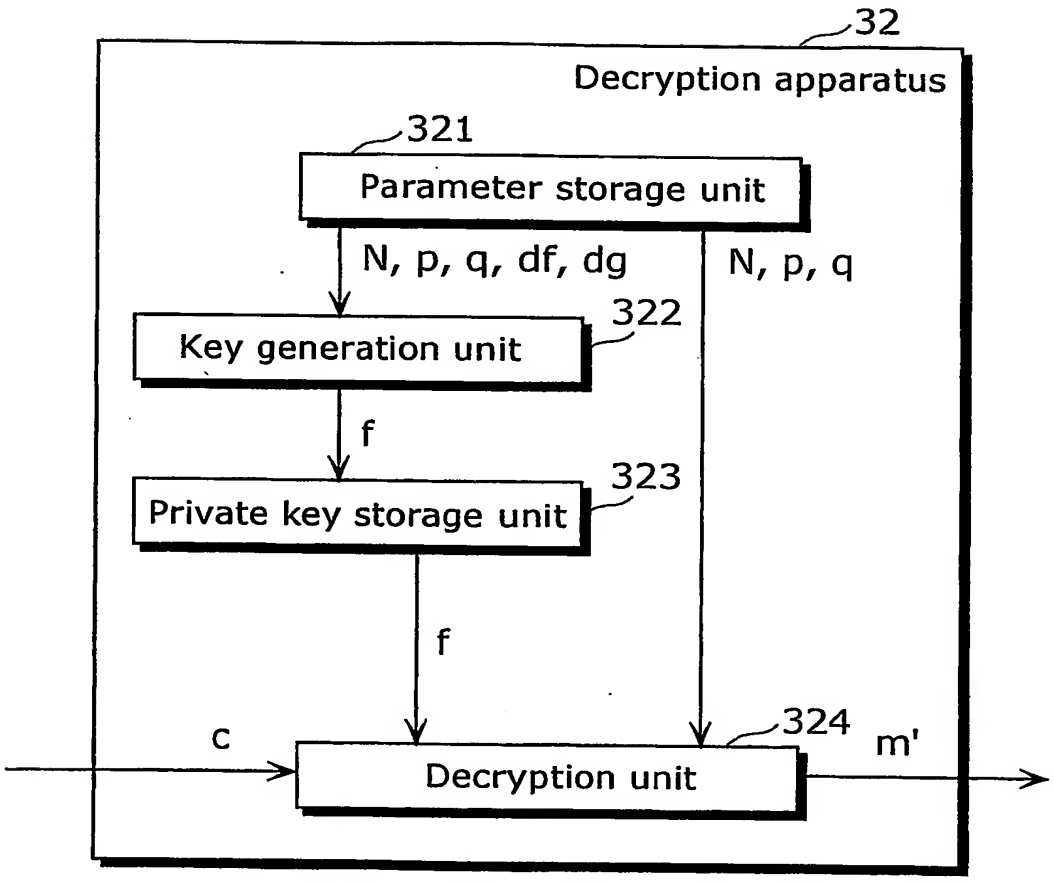

32
Decryption apparatus
321
Parameter storage unit
N, p, q, df, dg
N, p, q
322
Key generation unit
f
323
Private key storage unit
f
c
324
Decryption unit
m'

FIG. 14

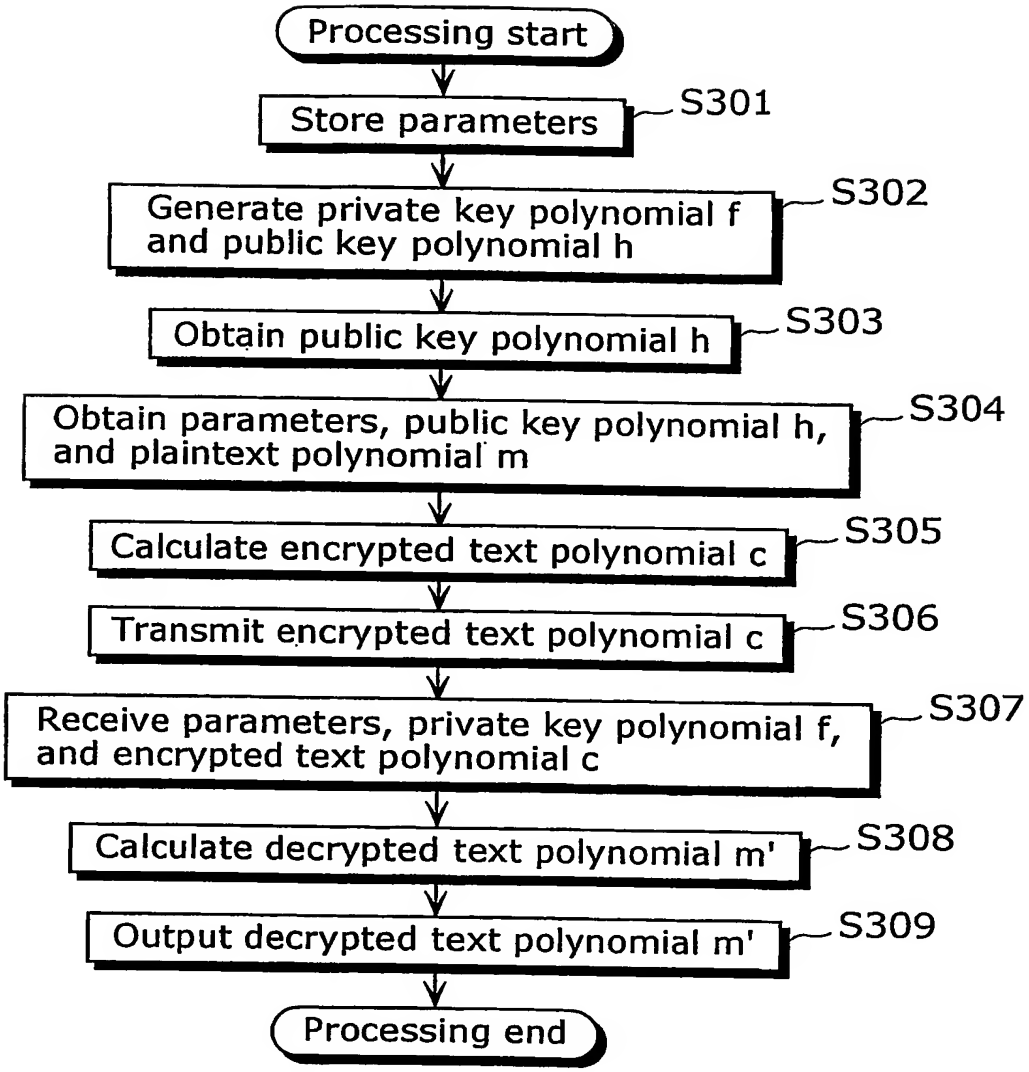

Processing start
Store parameters
S301
Generate private key polynomial f and public key polynomial h
S302
Obtain public key polynomial h
S303
Obtain parameters, public key polynomial h, and plaintext polynomial m
S304
Calculate encrypted text polynomial c
S305
Transmit encrypted text polynomial c
S306
Receive parameters, private key polynomial f, and encrypted text polynomial c
S307
Calculate decrypted text polynomial m'
S308
Output decrypted text polynomial m'
S309
Processing end

FIG. 15

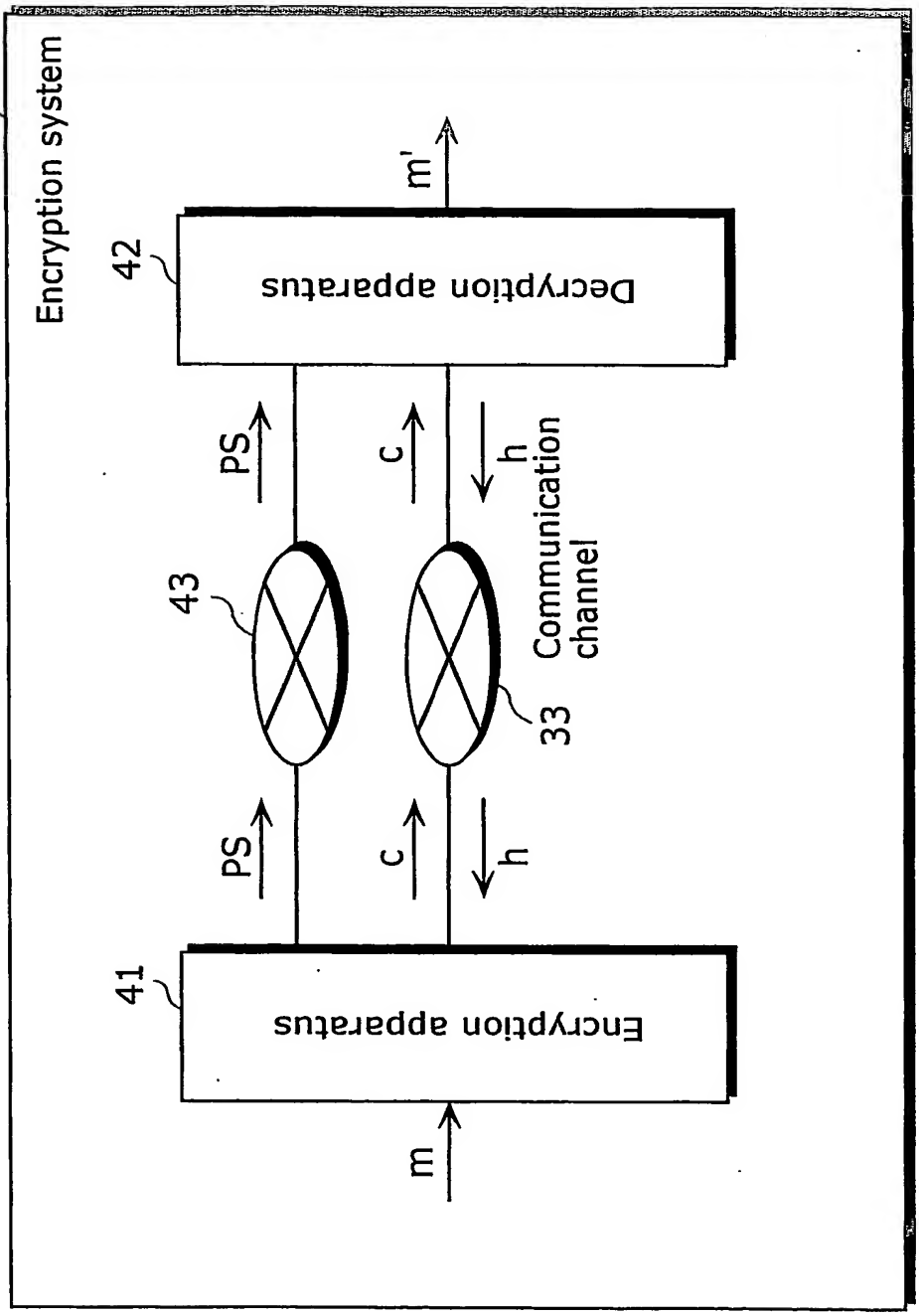

4
Encryption system
m'
42
Decryption apparatus
PS
c
h
Communication channel
43
33
PS
c
h
41
Encryption apparatus
m

FIG. 16

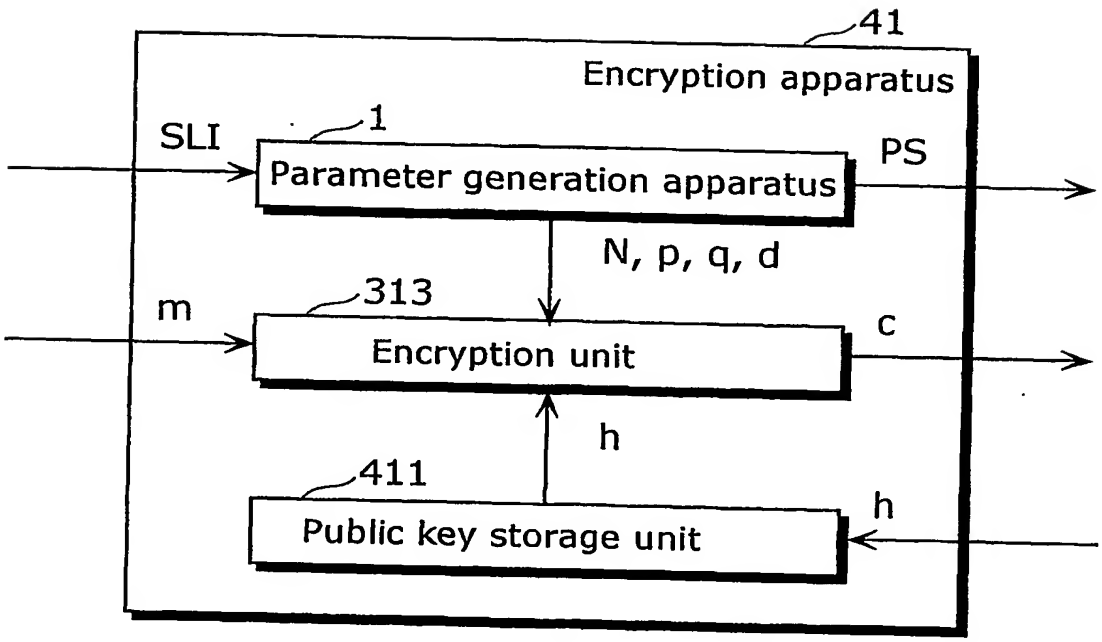

41
Encryption apparatus
SLI
1
Parameter generation apparatus
PS
N, p, q, d
m
313
Encryption unit
c
h
411
Public key storage unit
h

FIG. 17

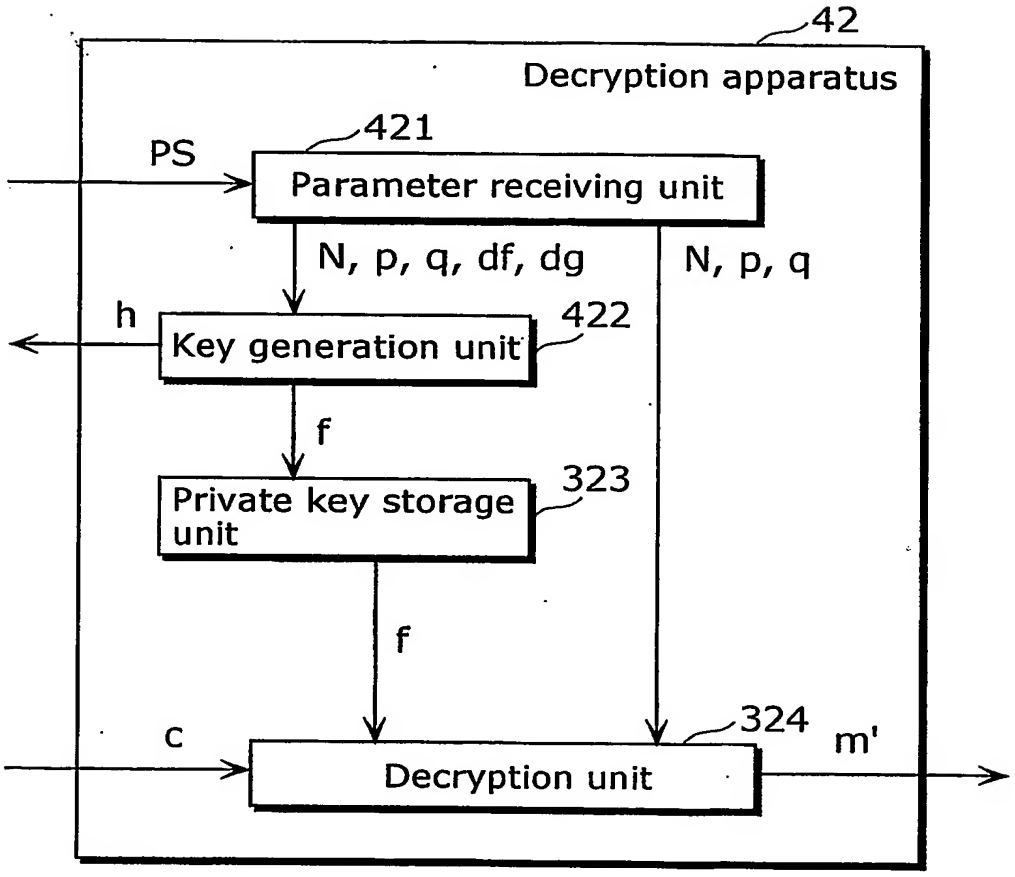
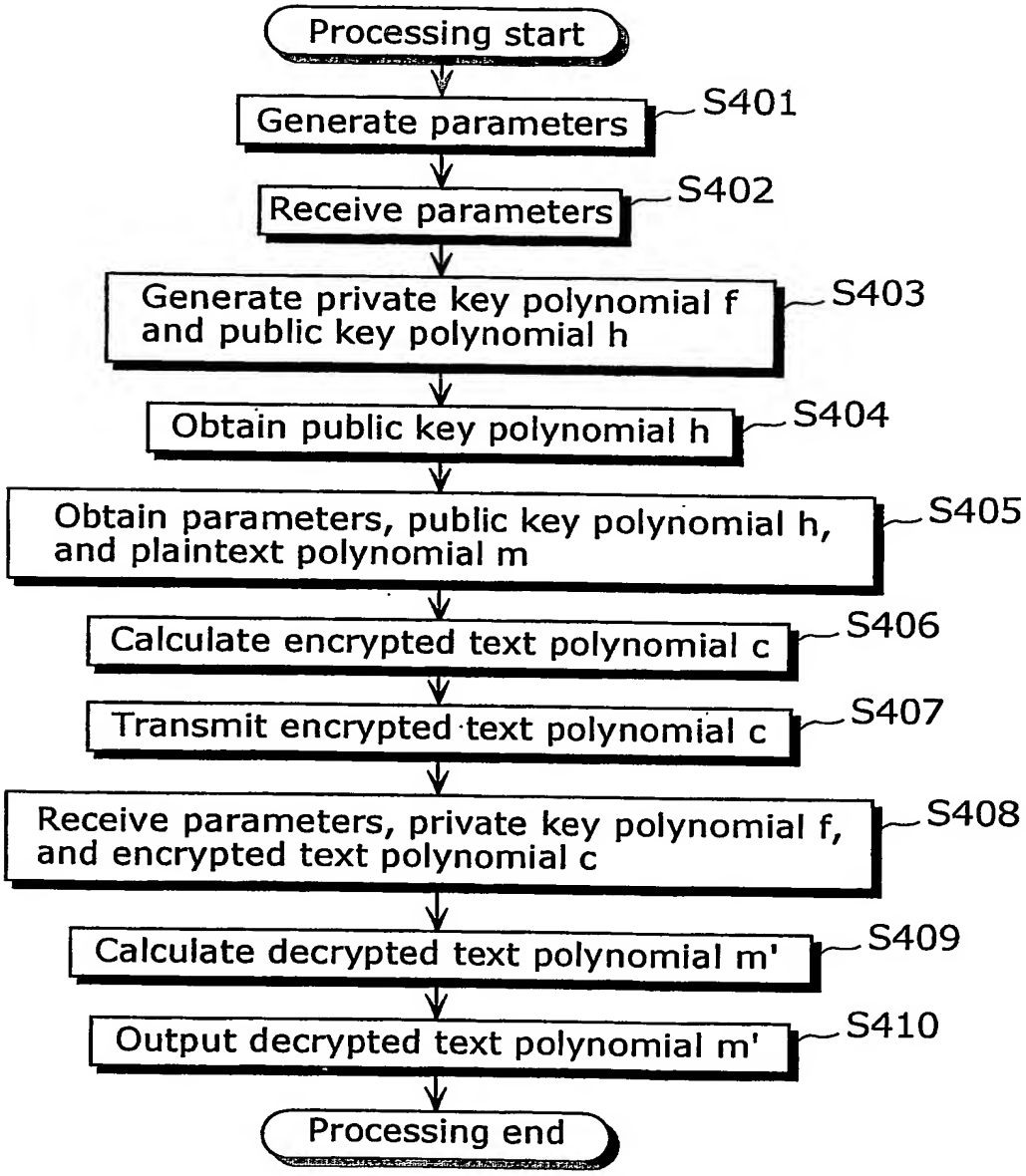

42
Decryption apparatus
421
PS
Parameter receiving unit
N, p, q, df, dg
N, p, q
h
Key generation unit
422
f
Private key storage unit
323
f
c
324
m'
Decryption unit

FIG. 18


Processing start
Generate parameters
S401
Receive parameters
S402
Generate private key polynomial f and public key polynomial h
S403
Obtain public key polynomial h
S404
Obtain parameters, public key polynomial h, and plaintext polynomial m
S405
Calculate encrypted text polynomial c
S406
Transmit encrypted text polynomial c
S407
Receive parameters, private key polynomial f, and encrypted text polynomial c
S408
Calculate decrypted text polynomial m'
S409
Output decrypted text polynomial m'
S410
Processing end